Notice of Allowability	Application No.	Applicant(s)	
	09/665,018	TAYLOR ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *RCE filed on 7/26/06 and Interview held on 9/28/2006*.

2. ☒ The allowed claim(s) is/are *1-3, 5-15, and 17-20*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *20060929* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

09/29/06

DETAILED ACTION

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Steven Wigmore and correspondence received via E-mail on September 29, 2006 (see attached). The application has been amended as follows:

1. (Currently Amended) A computer-implemented process for assessing the vulnerability of a workstation to a security compromise, comprising the steps:

issuing a request for a scanner from a browser operating on the workstation to a network server via a computer network;

transmitting the scanner from the network server to the workstation via the computer network, the scanner installable within the browser and operative to complete a vulnerability assessment of the workstation to identify security vulnerabilities of the workstation that can compromise secure operation of the workstation on the computer network;

completing a repair operation by the scanner to address a security vulnerability identified by the scanner in response to completing the vulnerability assessment of the workstation;

generating workstation credentials derived from the scanner conducting the vulnerability assessment of the workstation, the workstation credentials comprising at least one of information about integrity of the workstation and a security posture of the workstation;

comparing the workstation credentials to a workstation policy;

authenticating a workstation for access to the network server by granting the workstation access to one or more services available on the network server if the workstation credentials derived from the scanner are in compliance with the workstation policy;

if access to the one or more services available on the network server is granted to the workstation because the workstation credentials are in compliance with the workstation policy, issuing a request for credentials associated with a user; receiving credentials associated with a user; and authenticating a user of the workstation for access to the network server after said authenticating the workstation for access to the network server by determining if the user is authorized to access the one or more services available on the network server through evaluating the credentials associated with the user; and

if the workstation credentials do not match the workstation security policy, then denying access to the one or more network services.

4. (Cancelled).

8. (Currently Amended) A computer-implemented process for authenticating a workstation requesting a software service, comprising the steps:

issuing a request for a scanner to a network server from a browser operating on the workstation;

transmitting the scanner and a workstation policy from the network server to the workstation via the computer network, the scanner installable within the browser and operative to generate workstation credentials by completing a vulnerability assessment of the workstation, the workstation credentials comprising at least one of information about integrity of the workstation and a security posture of the workstation;

completing a repair operation by the scanner to address a security vulnerability identified by the scanner in response to completing the vulnerability assessment of the workstation;

comparing the workstation credentials to the workstation policy on the workstation to determine whether the workstation should be granted access to the software service;

authenticating a workstation for access to the software service by granting the workstation access to the software service available on the network server if the workstation credentials derived from the scanner are in compliance with the workstation policy; and

if access to the software service is granted to the workstation because the workstation credentials are in compliance with the workstation policy, authenticating a user of the workstation for access to the software service after said authenticating the workstation for access to the software service by issuing a request for user authentication in order to determine if a user of the workstation is authorized to access the software service available on the network server; and

if the workstation credentials do not match the workstation security policy, then denying access to the software service.

11. (Currently Amended) A computer-implemented process for authenticating a workstation requesting a network service from a network server via a computer network, comprising the steps:

issuing a request for a scanner to the network server from a browser operating on the workstation;

transmitting the scanner from the network server to the workstation via the computer network, the scanner installable within the browser and operative to generate workstation credentials by completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network, the workstation credentials comprising at least one of information about integrity of the workstation and a security posture of the workstation;

completing a repair operation by the scanner to address a security vulnerability identified by the scanner in response to completing the vulnerability assessment of the workstation;

transmitting the workstation security credentials from the scanner to the network server via the computer network;

determining at the network server whether the workstation should be granted access to a network service of the network based on the workstation credentials;

authenticating a workstation for access to the network service by granting the workstation access to the network service if the workstation credentials derived from the scanner are in compliance with the workstation policy; and

if access is granted to the workstation for the network service because the workstation credentials are in compliance with the workstation policy, authenticating a user of the workstation for access to the network service after said authenticating the workstation for access to the network service by issuing a request for information relating to user authentication in order to determine if the user is authorized to access the network service; and

if the workstation credentials do not match the workstation security policy, then denying access to the network service.

Reasons for Allowance

2. The following is an examiner's statement of reasons for allowance: The prior art of record US Patent Publication 2001/0034847 to Gaul, Jr. teaches method and apparatus for performing security vulnerability assessment which includes testing for vulnerabilities, storing any found vulnerabilities and correcting said found vulnerabilities. US Patent 6,438,600 to Greenfield et al teaches a method and system for securely sharing log-in credentials among trusted browser-based applications. Greenfield et al also teaches Requesting secure service from an executing applet, searching responsive to the request for stored credentials in a shared static data from which the shared static data area associated with the codebase from which executing applet is loaded and verifying stored credentials or new set of credentials before allowing the requested service to continue and performing the requested service if user is authorized. US Patent 6,298,445 to Shostack et al teaches assessing security vulnerabilities t provide security solutions to potential "weak" computer networks or computers. US Patent 6,418,472 to Mi et al teaches a system and method for controlling access to an object. A comparison agent is used to compare a value that may be compared with a processor identifier to determine whether the processor corresponds to the processor identifier and if the value matches then the computer grants the user access to the object. The prior arts of record, however, fail to teach singly or in combination: "issuing a request for a scanner from a browser operating on the workstation to a

network server via a computer network; transmitting the scanner from the network server to the workstation via the computer network, the scanner installable within the browser and operative to complete a vulnerability assessment of the workstation to identify security vulnerabilities of the workstation that can compromise secure operation of the workstation on the computer network; completing a repair operation by the scanner to address a security vulnerability identified by the scanner in response to completing the vulnerability assessment of the workstation; generating workstation credentials derived from the scanner conducting the vulnerability assessment of the workstation, the workstation credentials comprising at least one of information about integrity of the workstation and a security posture of the workstation; comparing the workstation credentials to a workstation policy; authenticating a workstation for access to the network server by granting the workstation access to one or more services available on the network server if the workstation credentials derived from the scanner are in compliance with the workstation policy; if access to the one or more services available on the network server is granted to the workstation because the workstation credentials are in compliance with the workstation policy, issuing a request for credentials associated with a user; receiving credentials associated with a user; and authenticating a user of the workstation for access to the network server after said authenticating the workstation for access to the network server by determining if the user is authorized to access the one or more services available on the network server through evaluating the credentials associated with the user; and if the workstation credentials do not match the workstation security policy, then denying access to the one or more network services" as recited in independent claim 1. Independent claims 8 and 11 recite similar process. Consequently, independent claims 1, 8, and 11 are allowable over the prior arts of record. Claims 2, 3, 5-7, 9-10, 12-15, 17-20 are directly or indirectly dependent upon claims 1, 8, and 11, and therefore are also allowable over the prior arts of record.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

cc

Carl Colin
Patent Examiner
September 29, 2006

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

09/29/06